Order Code RL32594

CRS Report for Congress
Received through the CRS Web

Public Safety Communications Policy

Updated March 24, 2006

Linda K. Moore
Analyst in Telecommunications Policy
Resources, Science, and Industry Division

Public Safety Communications Policy

Summary

Since September 11, 2001, the effectiveness of America's communications capabilities in support of the information needs of first responders and other public safety workers has been a matter of concern to Congress. The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) included sections that responded to recommendations made by the 9/ll Commission, in its report of July 2004, and by others in recent years, regarding public safety communications. Most public safety advocates consider that the communications failures following the onslaught of Hurricane Katrina demonstrate that there is much still to be done to provide the United States with adequate communications capabilities in emergencies. Whereas bills introduced before Hurricane Katrina struck the Gulf Coast have tended to address public safety communications in broad terms, with an emphasis on funding and interoperability, recent bills have put more emphasis on infrastructure.

In response to Hurricane Katrina, Senator Joseph I. Lieberman introduced S. 1725, a bill, that expands a similar, earlier bill (S. 1274). The new bill gives equal weight to building a more robust infrastructure and to assuring interoperability. Senator John F. Kerry has introduced a bill that would look at developing a back-up system to assure resilient communications for emergency responders (S. 1703). Representative Reichert has introduced a bill (H.R. 4941) that would improve standards for equipment used for homeland security, including interoperable communications. Among hurricane reconstruction funding bills, one introduced by Senator Mary L. Landrieu would direct $600,000,000 specifically to a Louisiana state program that would upgrade emergency communication statewide (S. 1765). Other funding bills that cover communications include S. 1645 and S. 1762 (Senator Boxer), S. 2412 (Senator Biden) and H.R. 1323 (Representative Stupak). The Deficit Reduction Act of 2005 (P.L. 109-171) includes provisions for up to $1 billion for interoperable communications, as well as for improvements in 911 and emergency alert systems.

At the end of the 108th Congress, significant steps were taken by Congress regarding improvement in public safety communications, many of them in response to recommendations by the 9/11 Commission. Commission recommendations for action to improve communications and the testimony and comments of experts are used as the framework for this report in reviewing issues such as planning; spectrum availability; new technologies like smart radios (software-defined radio, SDR); funding; and longer term goals and concerns. The nature of the problem of how best to meet the nation's emergency communications needs has not changed, but the events of Hurricane Katrina raised the level of awareness of the problem, among the public and at every level of government. As a result, the second session of the 109th Congress is likely to continue to press for detailed responses and measures that could shape policy decisions going forward.

This report will be updated.

Contents

Background 1
Planning: Post Katrina 2
Issues for the 109th Congress 3
Accountability and Oversight 3
Leadership 4
Role of Military 4
Digital Television Transition and Public Safety Fund 5
Intelligence Reform and Terrorism Prevention Act 6
Spectrum Allocation 6
Improving Spectrum Capacity for Public Safety 6
Communications Support and Interoperability 9
Interoperability: SAFECOM 9
Interoperability: Integrated Wireless Network 10
Interoperability: First Responders 11
Emergency Communications: New Legislation 12
Proposed Legislation for Emergency Communications 12
Related Legislative Initiatives 14
High-Risk Urban Areas 14
Proposed Legislation for Urban Areas 15
Funding Programs, Selected Issues 15
Some Recommendations from the Public Safety Sector 16

Appendix I - Federal Administration 17
National Telecommunications and Information Administration 17
Federal Communications Commission 18
Homeland Security 18
Spectrum and Interoperability 19
Department of Homeland Security 19
National Response Plan 19
Office of Interoperability and Compatibility 19
SAFECOM 20
SAFECOM Strategy as an E-Government Initiative 23
Regional Technology Integration Initiative 25
National Incident Management System (NIMS) 26
Integrated Wireless Network 26
National Communications System 27
Other Coordinating Bodies 27

Public Safety Communications Policy

Background

Public safety agencies include the nation's first responders (such as firefighters, police officers, and ambulance services), 911 call center staff, and a number of local, state, federal—and sometimes regional—authorities. Communications, often wireless radios, are vital to these agencies' effectiveness and to the safety of their members and the public. Wireless technology requires radio frequency capacity in order to function, and existing wireless technology is designed to work within specified frequency ranges.

Different operations, different applications, different rules and standards, and different radio frequencies are among the problems first responders face in trying to communicate with each other. Interoperability, also referred to as compatibility or connectivity, refers to the capability for different systems to readily connect to each other. Facilitating interoperability has been a policy concern of public safety officials for a number of years.[1] However, public safety agencies—especially at the local level—tend to rely on vendors for technical expertise. Interoperable solutions, therefore, are often based on proprietary systems, limiting the scope of connectivity. One way to bypass the vendor-driven planning that characterizes, and limits, public safety communications could be to implement a national plan that encouraged resource-sharing. At the level of national policy for emergency planning and response, for example, goals for interoperability could include interchangeability, assuring that equipment from any agency, state, or community could be used to replace or supplement equipment in any area of the country, as needed.

Since September 11, 2001—when communications failures added to the horror of the day—achieving interoperability for public safety communications has become an important policy concern for Congress. The damage to communications infrastructure caused by Hurricane Katrina and subsequent flooding has revealed the extent to which the concerns of Congress, as expressed in legislation, have yet to be acted upon. Although many replacements for lost communications equipment were rushed to critical sites in the Gulf Coast states, they were usually different systems using different radio frequencies, with little or no capability for cross-communication. Although interoperability in communications is correctly perceived as a subset of the larger problem of providing comprehensive communications support, it is a pivotal solution. Interoperability provides redundancy and back-up capacity, key elements for a robust network. Some have suggested that the current

[1] Difficulties in communications after a major plane crash in the Potomac River in January 1982 is often cited as the impetus for expanding interoperability in the Capital Area.

definition widely used in discussing interoperability may be too general,[2] and that a fuller articulation of planning goals should be developed to guide policy. Many experts agree that—at this point in what can only be described as an ongoing crisis in communications capacity—a critical missing element is planning at the national level. In this view, national planning—whether undertaken at the federal level, through a consortium of states, or other means—is needed to transcend proprietary solutions and bring about consensus on common interfaces with uniform standards that permit full interoperability and interchangeability for newer, digital equipment.

Planning: Post Katrina

Federalization of emergency response for disasters or catastrophic events could become inevitable unless states and communities have adequate resources to act in a timely manner. Current disaster response plans of the Federal Emergency Management Agency (FEMA) are built on the assumption that local resources will be adequate after a disaster strikes until additional resources arrive. The destructive chaos that followed in the wake of Hurricanes Katrina and Rita revealed many weakness in current assumptions and plans, such as those in the National Response Plan and the National Incident Management System. Two critical pieces of infrastructure failed early on: electrical power and communications. A well-planned and robust emergency communications system should be sustainable at reasonable levels of operation even after electrical power is lost. Resources to sustain operations include back-up generators and fuel, redundant systems, self-healing networks, access to multiple communications channels, common radio frequencies for wireless communications, sufficient spectrum bandwidth to support communications needs, and the proper equipment and infrastructure to make it all work. As testimony before Congress has regularly substantiated, industry plans for disasters, prepares to the best of its capacity, and carries out the plans as needed;[3] similar levels of planning and capacity to respond need to be achieved for emergency communications (and other public safety services) in communities.[4]

Since September 11, 2001, Congress has passed important legislation to respond to problems revealed after the attacks on the World Trade Center and the Pentagon, including problems of communications at the disaster sites. Provisions of the Homeland Security Act of 2002 (P.L. 107-296) instruct the Department of Homeland

[2] One frequently-cited definition of interoperability has been provided by the government agency SAFECOM. "In general, interoperability refers to the ability of public safety emergency responders to work seamlessly with other systems or products without any special effort. Wireless communications interoperability specifically refers to the ability of public safety officials to share information via voice and data signals on demand, in real time, when needed, and as authorized." [http://www.safecomprogram.gov].

[3] For example, testimony from telecommunications executives at hearing of Senate, Committee on Commerce, Science and Transportation, "Communications in a Disaster," September 22, 2005.

[4] For example, testimony and comments at hearing of House of Representatives, Committee on Homeland Security, Subcommittee on Emergency Preparedness, Science, and Technology, "The State of Interoperable Communications: Perspectives from the Field," February 15, 2006.

Security (DHS) to address some of the issues concerning public safety communications in emergency preparedness and response and in providing critical infrastructure. Telecommunications for first responders is mentioned in several sections, with specific emphasis on technology for interoperability.[5] Acting on recommendations made by the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), Congress included several sections regarding improvements in communications capacity—including clarifications to the Homeland Security Act—in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). These recommendations and some approaches to their implementation are the main topics of this report.

Issues for the 109th Congress

By requirements it included in the Intelligence Reform and Terrorism Act—for studies on interoperability strategies, use of technology, spectrum use, and more—Congress has assigned itself a number of specific tasks of oversight regarding emergency communications. Congress also has recognized the many dilemmas faced by its constituents in supporting communications interoperability. It has in many ways taken on the role of champion in support of programs for interoperability that benefit local communities, states and tribes. Some steps have been taken, particularly within DHS, and Congress has demanded further advances.[6] Despite indications of progress, much remains to be done. Issues that could be addressed—collectively or singly—by Congress, the Administration, the private sector, or others include the development of a long term strategy that coordinates both public safety spectrum needs and interoperable communications needs, and the coordination of the various studies requested by Congress and by the Administration. The findings and recommendations from these studies are crucial to the advancement of policy for public safety.

Accountability and Oversight. The achievement of a comprehensive set of solutions for interoperability outside the federal government's own communications needs appears to remain elusive. Participation of the federal government in a national solution for interoperability does not necessarily require federal ownership. The federal government is an important component, however, of any network that might be put in place to provide interoperable communications. In light of the critical role of federal participation, Congress could decide to extend its oversight role; proposed legislation also includes provisions that set higher standards for performance from federal agencies, notably the Department of Homeland Security. The first of several planned Congressional investigations into shortcomings in planning and response for disasters such as Hurricane Katrina has been published.[7]

[5] Notably, P.L. 107-296, Sec. 201. and Sec. 502.

[6] See for example, comments and questions of members during hearing of the House of Representatives, Committee on Homeland Security, Subcommittee on Emergency Preparedness, Science and Technology, "Ensuring Operability During Catastrophic Events," October 26, 2005.

[7] "A Failure of Initiative: The Final Report of the Select Bipartisan Committee to (continued...)

The administration also has released an account of the federal response to the disaster.[8]

Leadership. The devastation caused by the 2005 hurricane season, especially the impact of Hurricane Katrina on the Gulf Coast states, brought home to many how large the gap is between intentions and execution. As noted in another CRS report,[9] after FEMA was absorbed by DHS it was effectively "stripped" of responsibilities for planning for emergency communications. The leadership role for preparing a national strategy for communications interoperability was assigned to the Office of Interoperability and Compatibility within DHS, resting primarily with the SAFECOM program. The decision was made at the executive level that SAFECOM would be the lead agency for communications interoperability, a position that was strengthened by organizational changes within DHS, and ratified by Congress with the passage of the Intelligence Reform and Terrorism Prevention Act.

Role of Military.[10] The 9/11 Commission has proposed using a signal corps solution to improve communications capacity, without elaborating on how this might be achieved. (Some information on signal corps organization and technology appears later in this report.) Many experts familiar with the macro-level concepts of signal corps communications support suggest that one approach for public safety could be to upgrade the type of emergency communications equipment that can be brought to a disaster site so that it resembles the far-reaching capabilities and capacity of the Army Signal Corps yet is readily accessible to local first responders and other officials "on the ground." In many situations, search and rescue teams in New Orleans and other devastated communities could not communicate with each other because their radios did not use the same frequencies. The difficulties in coordination placed an extra burden on relief efforts. Rescue efforts improved after military forces arrived in part because of their units' superior communications resources. Effective command-and-control operations depend on communications links. Just as the 9/11 Commission looked at the Army Signal Corps as a possible resource for improving interoperable communications, many are now weighing the possibility of giving a greater role to the military for emergency response within the United States. Bottom line, in this view, today the military has the communications equipment to do the job of emergency response while FEMA, the states, and first responders do not.[11] The

[7] (...continued)
Investigate the Preparation for and Response to Hurricane Katrina," House of Representatives, February 12, 2006.

[8] "The Federal Response to Hurricane Katrina" Lessons Learned," report to the President, Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism, February 23, 2006.

[9] CRS Report RL33064, *Organization and Mission of the Emergency Preparedness and Response Directorate: Issues and Options for the 109th Congress*, by Keith Bea.

[10] Information on response capabilities is in CRS Report RL33095, *Hurricane Katrina: DOD Disaster Response*, by Steve Bowman et al.

[11] The military is generally perceived to have cutting-edge communications technology and clear chains of command for the technology. A survey of perceptions of capacity at the state (continued...)

technology exists, but it has not been deployed at meaningful levels. Although the stories of the failures in organization in responding to disasters on the Gulf Coast are legion, in the area of emergency communications it was usually the inadequate technology that failed first, not the people.

Digital Television Transition and Public Safety Fund. The Balanced Budget Act of 1997 requires the FCC to allocate 24 MHz of spectrum at 700 MHz[12] to public safety, without providing a hard deadline for the transfer.[13] The channels designated for public safety are among those currently held by TV broadcasters; they are to be cleared as part of the move from analog to digital television (DTV). The 9/11 Commission urged that Congress take prompt action to assure the release of spectrum at 700 MHz—allocated for public safety, but not released—to support needed interoperable network and more robust communications capacity. Provisions in the Deficit Reduction Act (P.L. 109-171) plan for the release of spectrum by February 18, 2009[14] and would create a fund to receive spectrum auction proceeds and disburse designated sums to the Treasury and for other purposes.[15] $7,363 million from these auctions would go to reduce the budget deficit as specified in H.Con.Res. 95.[16] Other disbursements from the fund include a grant program of up to $1,000 million for public safety agencies to deploy systems on 700 MHz spectrum they will receive as part of the transition.[17] The fund and disbursements are to be administered by the National Telecommunications and Information Administration (NTIA).

Effective October 1, 2006, the NTIA will be able to borrow funds for communications interoperability grants. The Congressional Budget Office anticipates that the grants program will receive $100 million in FY2007, $370 million in 2008, $310 million in 2009 and $220 million in 2010.[18] The grants are to go for interoperability programs that use or are interoperable with communications

[11] (...continued)
and local level is being compiled in the SAFECOM Interoperability Baseline Survey.

[12] Radio frequency spectrum is measured in hertz. Radio frequency is the portion of electromagnetic spectrum that carries radio waves. The distance an energy wave takes to complete one cycle is its wavelength. Frequency is the number of wavelengths measured at a given point per unit of time, in cycles per second, or hertz (Hz). Typical designations are: kHz—kilohertz or thousands of hertz; MHz—megahertz, or millions of hertz; and GHz —gigahertz, or billions of hertz.

[13] 47 U.S.C. § 309 (j) (14).

[14] S. 1932, Sec. 3002 (a) (1) (B).

[15] S. 1932, Sec. 3004 (3) "(E) "(I) and (ii).

[16] S. 1932, Sec. 3004 (3) "(E) "(iii).

[17] S. 1932, Sec. 3006.

[18] Congressional Budget Office Cost Estimate, S. 1932, Deficit Reduction Act of 2005, January 27, 2006, p. 21, [http://www.cbo.gov/showdoc.cfm?index=7028&sequence=0].

systems that can work at 700 MHz.[19] The act also requires the release of spectrum by February 2009. For the funds to be used effectively, therefore, states would benefit from completed plans for using 700 MHz. Although there are a number of provisions for funding programs for communications and planning, none of the existing programs is designed to profit from the new grants program.

Intelligence Reform and Terrorism Prevention Act

The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) analysis of communications difficulties on September 11, 2001 was summarized in the following recommendation.

> Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress.[20]

The Commission, in this paragraph, recognized the important link between access to spectrum and the effectiveness of communications technology. Briefly, the recommendation says:

- free up and assign more **spectrum** for public safety use;
- establish **communications support** (the role of a signal corps typically is to provide information systems and networks for real-time command and control);
- with **interoperable communications** (connectivity); and
- prioritize funding these communications operations for **high-risk urban areas**.

Spectrum Allocation

With the passage of the Deficit Reduction Act, Congress has achieved an important milestone in providing a date certain for the release of spectrum for pubic safety use.[21] This spectrum will provide what is known as "green space," unoccupied frequencies that can be used to support new systems without disrupting operations on other radio frequency waves.

Improving Spectrum Capacity for Public Safety. The Intelligence Reform and Terrorism Prevention Act requires the FCC, in consultation with the Secretary of Homeland Security and the National Telecommunications and

[19] S. 1932, Sec. 3006 (a) (1) and (d) (3).

[20] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (Washington: GPO, 2004), p. 397.

[21] February 18, 2009. S. 1932, Sec. 3002 (a) (1) (B).

Information Administration (NTIA),[22] to conduct a study on the spectrum needs for public safety, including the possibility of increasing the amount of spectrum at 700 MHz.[23] This provision is responsive to the many public safety officials who believe that additional spectrum should be assigned for public safety use—and not exclusively for first responders.[24] In addition to providing spectrum for other types of users, the spectrum available for public safety should be able to support high-speed transmissions capable of quickly sending data (such as photographs, floor plans and live video). This requires providing frequencies with greater bandwidth to enable wireless broadband and new-generation technologies. Although radio frequencies have been designated for state and local public safety use in the 700 MHz range, there are no allocations specifically for federal use at 700 MHz and the bandwidth assignments are judged by most experts to be too narrow for full broadband. Many have advocated that additional spectrum be allocated at 700 MHz to accommodate federal users and to support newer, broadband wireless technologies as part of a nationwide network for public safety communications. The Spectrum Coalition for Public Safety has circulated proposed legislation that would allocate additional spectrum at 700 MHz for use by state and local first responders, critical infrastructure industries, and federal public safety agencies.[25]

In the study requested by Congress, the FCC sought comment on whether additional spectrum should be made available for public safety, possibly from the 700 MHz band. Comments received from the public safety community overwhelmingly supported the need for additional spectrum, although other bands besides 700 MHz were also mentioned. The FCC did not make a specific recommendation for additional spectrum allocations in the short-term although it stated that it agreed that public safety "could make use of such an allocation in the long-term to provide broadband services."[26] It qualified this statement by observing that spectrum is only one factor in assuring access to mobile broadband services for emergency response. It further announced that it would move expeditiously to see whether the current band plan for the 24 MHz at 700 MHz currently designated for public safety could be

[22] The NTIA, Department of Commerce, administers federal use of spectrum.

[23] P.L. 108-458, Title VII, Subtitle E, Sec. 7502 (a).

[24] In 1997 amendments to the Communications Act of 1934 , Congress defined public safety services as "services—(A) the sole or principal purpose of which is to protect the safety of life, health or property; (B) that are provided (i) by State or local government entities; or (ii) by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services ; and (C) that are not made commercially available to the public by the provider." [47 U.S.C. § 337 (f)(1)]. The Intelligence Reform and Terrorism Prevention Act uses the more restrictive definition of first responders as provided in the Homeland Security Act of 2002 (6 U.S.C. § 101).

[25] Spectrum Coalition for Public Safety at [http://www.spectrumcoalition.dc.gov/html/home.html].

[26] *Report to Congress on the Study to Assess Short-term and Long-term Needs for Allocations of Additional Portions of the Electromagnetic Spectrum for Federal, State and Lxcal Emergency Response Providers,* Federal Communications Commission, December 19, 2005, paragraph 99, at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-262865A1.pdf]. Viewed December 27, 2005.

modified to accommodate broadband applications.[27] On March 17, 2006, the FCC issued a request for comment on a new band plan that would allocate spectrum for broadband use by first responders within the 24 MHz currently assigned for public safety. The same proposed rulemaking also asks for additional comment on the possible adaptation of a wireless broadband standard for interoerability.[28]

Although, cumulatively, radio frequencies designated for non-federal public safety total over 90 MHz,[29] the characteristics of these frequencies are dis-similar, requiring different technological solutions. The fragmentation of spectrum assignments for public safety is a significant barrier to achieving interoperability in the future, and is presently among the technical problems that plague public safety communications, such as out-of-date equipment, proprietary solutions, congestion, and interference. The immediate barrier to achieving radio communications interoperability is—simply put—that UHF and VHF frequencies[30] cannot connect directly with each other, and that older, analog equipment widely used below 512 MHz cannot connect with newer digital equipment at 800 MHz. Technology for new frequencies at 4.9 GHz is still in the early stage of development but these frequencies appear suitable primarily for local-area (short-range) transmission. None of the above frequency assignments can, using current technology, support wide-area communications relying on high-speed, data-rich transmissions. Providing new spectrum at 700 MHz for key communications capabilities, including interoperable connections, is viewed by many as the optimal solution for overcoming problems caused by incompatible radio frequencies and technologies.

The need for greater spectral capacity will grow with the number of participants in interoperable systems and the amounts of information being shared on these systems. Bottlenecks in communications are a problem that is already manifest among federal computer networks and landline transmissions, and many believe it will worsen as more information is pushed through. As emergency response units become more mobile, demand for time-critical, wireless communications capacity will also increase. New technologies that improve communications capacity are being introduced almost continuously, but the need to provide suitable spectrum for a full range of voice and data communications will persist.

[27] Ibid., paragraph 100.

[28] FCC, *Eighth Notice of Proposed Rule Making*, WT Docket 96-86, released March 17, 2006.

[29] Estimated at approximately 97 MHz in Testimony of Michael K. Powell, Chairman, Federal Communications Commission, at Hearing of Senate Committee on Commerce, Science and Transportation, "Spectrum for Public Safety Users," September 8, 2004. The NTIA has apparently not supplied a similar estimate of frequencies assigned to federal agencies that are or can be accessed for public safety purposes.

[30] Very High Frequency (VHF) operates in bands between 30 MHz to 300 MHz and Ultra High Frequency (UHF) operates in bands between 300 MHz and 3 GHz.

Communications Support and Interoperability

The 9/11 Commission recommendation to use signal corps to assure connectivity in high-risk areas is apparently a reference to the Army Signal Corps. In testimony before Congress, Commissioner John F. Lehman commented on the lack of connectivity for first responders and referred to the "tremendous expertise" of the Department of Defense (DOD) and its capabilities in procurement, technology, and research and development. Referring specifically to the Army Signal Corps, Mr. Lehman suggested that the DOD should have responsibility to provide "that kind of support to the first responders in the high-target, high risk cities like New York."[31]

The role of a signal corps typically is to provide information systems and networks for real-time command and control. The Army maintains mobile units to provide capacity and specialized support to military operations, worldwide. According to the U.S. Army Info Site on the Internet

> The mission of the Signal Corps is to provide and manage communications and information systems support for the command and control of combined arms forces. Signal support includes Network Operations (information assurance, information dissemination management, and network management) and management of the electromagnetic spectrum. Signal support encompasses all aspects of designing, installing, maintaining, and managing information networks to include communications links, computers, and other components of local and wide area networks. Signal forces plan, install, operate, and maintain voice and data communications networks that employ single and multi-channel satellite, tropospheric scatter, terrestrial microwave, switching, messaging, video-teleconferencing, visual information, and other related systems. They integrate tactical, strategic and sustaining base communications, information processing and management systems into a seamless global information network that supports knowledge dominance for Army, joint and coalition operations.[32]

The Army Signal Corps is intended to provide a communications backbone, a core network, with important elements such as spectrum management, the operation of communications centers, and support of communications networks that include both large area regional communications and radio coverage for local wireless interoperability. The Corps' communication backbone delivers connectivity on site among combined forces and connectivity to command centers. These operations are scalable and can be deployed when and where needed.

Interoperability: SAFECOM. Responsibility to coordinate and rationalize federal networks, and to support interoperability, has been assigned to SAFECOM by the Office of Management and Budget (OMB) as an e-government initiative. This

[31] Testimony of Commissioner John F. Lehman, National Commission on Terrorist Attacks Upon the United States, Hearing, House of Representatives, Committee on Government Reform, "Moving from 'Need to Know' to 'Need to Share,'" August 3, 2004.

[32] From [http://www.us-army-info.com/pages/mos/signal/signal.html]. Viewed October 13, 2005.

role has been supported by the Administration[33] and confirmed by Congress with language in the National Intelligence and Terrorism Prevention Act.[34] Programs at SAFECOM, now placed within the DHS Office for Interoperability and Compatibility, are primarily consultative in nature and focused on administrative issues. While it makes important contributions to testing equipment and working on technical and operational standards for interoperable equipment, SAFECOM does not appear to be planning for a standardized approach that can encompass state networks for public safety communications.

Interoperability: Integrated Wireless Network. Separately, an Integrated Wireless Network (IWN) for law enforcement is being planned as a joint program by the Departments of Justice, the Treasury, and Homeland Security. DHS is represented in the IWN Joint Program Office through the Wireless Management Office of the Chief Information Officer.[35] IWN, from its description, will have limited interoperability at the state and local level. The described objective of IWN is network integration for "the nation's law enforcement wireless communication, and data exchange capability through the use of a secure integrated wireless network."[36] Most of the parameters of the IWN program—equipment, technologies, standards, use of spectrum, etc.—will be established through the final choice of vendor or vendors and the network solutions proposed. There are some specific requirements, such as for open standards or standards that are readily available to all —such as Project 25—[37] and use of VHF frequencies already assigned to federal users.[38] Currently, the program has selected five companies as semi-finalists.[39] These companies have been asked to submit a detailed system design and an implementation plan[40] and are encouraged to provide "innovative, big-picture,

[33] Testimony of Karen S. Evans, E-Gov/IT Director, Office of Management and Budget, Hearing of the House of Representatives, Committee on Government Reform, Joint Hearing, Subcommittee on National Security, Emerging Threats and International Relations and Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "Public Safety Interoperability: Can You Hear Me Now?," Nov. 6, 2003.

[34] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (a) (2).

[35] Memorandum of Understanding Between the Department of Homeland Security, the Department of Justice, and the Department of the Treasury Regarding a Joint Tactical Wireless Communications System, at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

[36] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.3 (a), p. 8 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

[37] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.1 (d), p. 8 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

[38] Presentation by Michael Duffy, Deputy Chief Information Officer, E-Gov, Department of Justice, at Integrated Wireless Network (IWN) Industry Day, April 27, 2004.

[39] They are: AT&T, Boeing, General Dynamics, Lockheed Martin and Motorola. From Results of the IWN Phase I Downselect at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

[40] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, A.4 (a), p. 3 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

solution sets."[41] The departmental objectives for coverage are: major metropolitan areas; major highways; U.S. land and sea border areas; and ports of entry.[42] The reported estimated cost for IWN is $10 billion.[43] Funding is provided jointly from budgeted sums designated for the upgrading of communications equipment to meet NTIA requirements for narrowbanding and interoperability.[44] Although the network being sought is intended to serve law enforcement users within the three sponsoring departments, descriptions of the program invoke the possibility that IWN will provide the template for national interoperability.[45]

Interoperability: First Responders. In terms of achieving interoperability for the nation's first responders, the deployment of IWN could be viewed by some as a glass that is either half empty or half full. Among the positive contributions that IWN will provide to public safety communications are: the eventual adoption, on a massive scale, of a network architecture that can be emulated by all—presumedly with standardized interfaces; coordination of communications and interoperability among important components of homeland security; and significant improvements in communications technology and the efficient use of spectrum.

There could be questions as to how this project, running parallel with plans from the Office of Interoperability and Compatibility, will impact the goal that Congress has set for nationwide interoperability. Will it, for example, delay work on standards development until the process of vendor selection is complete and the standards for IWN have been fully established? Will the proposed interface between federal law enforcement personnel and selected state and local officials be extendable to, say, interoperability between those officials and local firefighters or EMS personnel? Should other federal networks be built along functional lines and then linked with IWN, possibly providing the connectivity needed at the state and local level among different types of responders? Will there be a link to emergency alert and warning systems? Could IWN serve as a connecting link between state and local first responder networks and the military. The specification to use federal frequencies apparently solves the problem of spectrum access for IWN but does not appear to move toward the solution to the vexing problem of providing suitable radio frequencies for interoperability for first responders. The frequencies that IWN is to

[41] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.1(c), p. 7 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

[42] Ibid.

[43] "Massive Federal Wireless Project Delayed," by Wilson P. Dizard III, GCN, March 30, 2005.

[44] Memorandum of Understanding Between the Department of Homeland Security, the Department of Justice, and the Department of the Treasury Regarding a Joint Tactical Wireless Communications System, and Presentation by Michael Duffy, Deputy Chief Information Officer, E-Gov, Department of Justice, at Integrated Wireless Network (IWN) Industry Day, April 27, 2004.

[45] "The successful deployment and operation of IWN will be a key enabler for national coordination capability," in Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.5 (b) (1), p. 10 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

use are the same frequencies that were generally not available to those responding to terrorist attacks on September 11, 2001.

Emergency Communications: New Legislation

Congress responded to recommendations for improvements in programs to support communications and foster interoperability with language in the Intelligence Reform and Terrorism Prevention Act that raises the bar for performance and accountability, as well as easing some of the obstacles to performance.[46] Among the program goals the act sets for the Department of Homeland Security and the Federal Communications Commission are the following.

- Develop a comprehensive, national approach for achieving interoperability.
- Coordinate with other federal agencies.
- Establish appropriate minimum capabilities for interoperability.
- Accelerate development of voluntary standards.
- Encourage open architecture and commercial products.
- Assist other agencies with research and development.
- Prioritize within DHS for research, development, testing and related programs.
- Establish coordinated guidance for federal grant programs.
- Provide technical assistance.
- Develop and disseminate best practices.
- Establish performance measurements and milestones for systematic measurement of progress.[47]

Proposed Legislation for Emergency Communications. Responding to the catastrophic failure of emergency communications in Gulf Coast States after the passage of Hurricane Katrina, Senator Joseph I. Lieberman presented a broad-based bill for changes in management of emergency communications within the Department of Homeland Security. Some of the elements of S. 1725 were in an earlier bill, S. 1274, introduced by the Senator in June 2005. S. 1725 was passed by the Committee on Homeland Security and Governmental Affairs on September 22, 2005 and reported, as amended in mark up, to the Senate on September 29 by Senator Susan M. Collins.

The thrust of S. 1725, the Assure Emergency and Interoperable Communications for First Responders Act of 2005, as reported, is to raise the level of accountability by DHS for the performance of emergency communications by expanding the department's responsibilities and by providing more detail about what is to be accomplished. The option of creating an Office for Interoperability and Compatibility within DHS that is part of P.L. 108-458[48] would be amended to become a requirement for an Office of Emergency Communications, Interoperability

[46] A discussion of federal programs is included in the **Appendix** of this report.

[47] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (a) (1).

[48] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (a) (2).

and Compatibility. Among the responsibilities specified for the office would be: to conduct extensive outreach programs nationwide for the improvement of emergency communications; to coordinate with the National Communication System; to develop a national strategy; to develop a national architecture that "defines components of an interoperable system and how they fit together; to set up a task force with broad responsibilities; to work with the Office of Domestic Preparedness in helping to create regional task forces, among other goals, and in funding and conducting a number of pilot programs. Goals of the pilot programs include testing new technology in a real-world environment; encouraging more efficient use of existing resources; and testing and deploying more robust and effective public safety communications systems. Other responsibilities of the office encompass working with the private sector to develop solutions to improve communications and interoperability; to use modeling and simulation for training exercises and to develop command-and-control functionality; and to take all necessary steps to improve emergency communications capabilities and to achieve communications interoperability.

The bill would amend the definition of "Interoperable Communications" as it appears in P.L.108-458[49] to read "Interoperable Communications and Communications Interoperability," and adds a definition for "Emergency Communications Capabilities." This term describes the uninterrupted flow of information to emergency responders at all levels, even after significant loss of capacity and critical infrastructure.[50]

Other provisions in the bill that reaffirm or slightly modify provisions passed as part of P.L. 108-458, include sections on pilot programs for communications in high-risk urban areas,[51] for collaboration with the Department of Defense in research and development,[52] and in requirements for states in order to qualify for funding.[53] S. 1725 would establish a panel to work with the Office of Domestic Preparedness in reviewing grants. The review panel would include members with technical expertise in emergency communications and interoperability as well as emergency response providers.

Evaluating the need for more robust emergency communications system, Senator John F. Kerry has proposed the Communications Security Act (S. 1703). The bill would amend the Homeland Security Act to require a study by DHS and the FCC of "the technical feasibility of creating a back-up emergency communications system that complements existing communications resources and takes into account next generation and advanced telecommunications technologies." Among the technologies to be considered are satellite connections. The language of the bill

[49] Sec. 7303 (g) (1).

[50] S. 1725, Sec. 3 (b).

[51] S. 1725, 'Sec. 316 would amend Title II, Homeland Security Act. Similar language appears in P.L. 108-458, Sec. 7304

[52] S. 1725, 'Sec. 314, '(b). A recommendation to consult DOD for development of pilot projects is in P.L. 108-458, Sec. 7304 (d).

[53] S. 1725, Sec. 107 and P.L. 108-458, Sec. 7303 (f).

would equip all public safety entities with the necessary equipment, this could be interpreted to include 911 call centers, an important part of the emergency communications safety net.

The need to improve standards and accelerate their development is addressed in a bill by Representative David G. Reichert (H.R. 4941). The Homeland Security Science and Technology Enhancement Act would require the Department of Homeland Security to take actions to support the development of standards consistent with voluntarily developed standards in a number of categories related to homeland security; interoperable communications for wireless and wireline networks is among these categories. Standards for training, including planning and joint exercises would also be addressed. Other sections of the bill deal with technology development and transfer, the Homeland Security Institute, the Homeland Security Technology Advisory Committee, the Regional Technology Integration Program, cybersecurity research and development, standards for critical infrastructure information systems, scholarship and fellowship programs, and a demonstration program for surveillance cameras.

Related Legislative Initiatives

High-Risk Urban Areas. The 9/11 Commission recommendation urged immediate funding of signal corps in high-risk urban areas to assure connectivity "among civilian authorities, local first responders, and the National Guard." The act responded by amending the Homeland Security Act to specify that DHS is to give priority to the rapid establishment of interoperable capacity in urban and other areas determined to be at high risk from terrorist attack. The Secretary of Homeland Security is required to work with the FCC, the Secretary of Defense, and appropriate state and local authorities to provide technical guidance, training, and other assistance as appropriate.[54] Minimum capabilities for "all levels of government agencies," first responders, and others include the ability to communicate with each other and to have "appropriate and timely access" to the Information Sharing Environment, an initiative treated elsewhere in the act.[55]

The act further requires the Secretary of Homeland Security to establish at least two pilot programs in high threat areas. The process of development for these programs is to contribute to the creation and implementation of a national model strategic plan.[56] The purpose of this plan is to foster interagency communications at all levels of the response effort.[57] Building on the 9/11 Commission recommendation to use the resources of the Army Signal Corps, the Secretary is to consult with the Secretary of Defense in the development of the pilot projects,

[54] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (d), 'Sec. 510 '(a).

[55] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (d), 'Sec. 510 '(b).

[56] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (a).

[57] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (b).

including review of standards, equipment, and protocols.[58] DHS was to have established at least two pilot projects in high threat or urban areas for interagency communications by March 2005;[59] as of the date of this report, this program is in review.

Proposed Legislation for Urban Areas. Underscoring the need to aid first responders in urban areas, H.R. 1795 (Representative Maloney) would require DHS to provide a communications system for the New York City Fire Department, including radios for the entire department and upgrades to its dispatch system. The bill specifies that such a network should be "seamless from the receipt of a 911 call to the dispatch of the firefighter," and interoperable with other public safety offices within the city. Other systems requirements include being able to transmit a firefighter's identity and location; sufficient capacity to send, in real time, data about buildings and property; performance tested for operation in "all locations and under all conditions in which firefighters can reasonably be expected to work...."

Funding Programs, Selected Issues. Grants that have helped to pay for new programs for interoperability have come from a number of federal sources, notably from Department of Justice programs and, within the Department of Homeland Security (DHS), from the Federal Emergency Management Administration (Emergency Preparedness and Response Directorate) and the Office for Domestic Preparedness (ODP) in the Border and Transportation Security Directorate. Grant programs such as those at ODP for Urban Area Security and High-Threat Urban Areas are on-going.[60]

A bill to offset proposed budget cuts in some of the funding programs, among other purposes, has been introduced by Senator Joseph R. Biden, Jr. The 9/11 Commission Recommendations Implementation Act (S. 2412) addresses a number of issues and proposals raised by the 9/11 Commission. First responders needs are addressed in the bill, primarily in authorizations to restore or increase funding to programs that pay for equipment, including the Urban Area Security Initiative Grant Program.

Provisions of the Intelligence Reform and Terrorism Prevention Act permit federal funding programs to make multi-year commitments for interoperable communications for up to three years, with a ceiling of $150 million for future

[58] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (d).

[59] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (a).

[60] For full details, please refer to CRS Report RS21677, *Office for Domestic Preparedness Grants for 2004: State Allocation Fact Sheet*; CRS Report RL32696, *Fiscal Year 2005 Homeland Security Grant Program: State Allocations and Issues for Congressional Oversight;* and CRS Report RS22050, *FY2006 Appropriations for State and Local Homeland Security*, all by Shawn Reese. A report from the Government Accountability Office provides many details about funding for first responders, especially grants from ODP: *Management of First Responder Grant Programs and Efforts to Improve Accountability Continue to Evolve*, April 12, 2005, GAO-05-530T.

obligations.[61] The act authorizes annual sums for a period of five years to be used for programs to improve interoperability and to assist interoperable capability in high-risk urban areas; the 2005 authorization is $22,105,000; the amount rises each year to $24,879,000 in 2009.

Some Recommendations from the Public Safety Sector

The debate about public safety communications and the role of federal policy is long running. The framework for current discussions—which accommodate recent advances in technology—most likely dates to a report in 1996 by the Public Safety Wireless Advisory Committee (PSWAC).[62]

Listed below are some key components of a desirable public safety communications policy for first responders described in the PSWAC study and in more recent reports, testimony, and other comments cited in this report. According to these sources, a national policy for public safety communications needs to address and correlate a myriad of complex goals, such as

- Coordinated assignment and use of spectrum at various frequencies.
- Muscular and sustained efforts to complete the development and application of technical and operational standards.
- Public sector adaptation of new technologies already available in the private sector such as for high-speed, data rich, and video or image transmissions.
- Long-term support of research and development for new technology.
- Coherent goals that encourage private investment in technology development.
- Nationwide network of communications operations centers (regional signal corps) that can serve as back-up facilities to each other and to state and interstate centers and networks.
- Interoperability of communications among first responders and public safety agencies.
- Managerial structure that can successfully coordinate not only disparate federal, state, and local agencies but also the different cultural and technical needs of independent first responder units.
- Framework to match policy goals with implementation needs to assure the effectiveness of federal funding for programs and grants.

[61] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (e).

[62] The Public Safety Wireless Advisory Committee (PSWAC) was chartered in 1995, at the request of Congress, to study public safety spectrum and make recommendations for meeting spectrum needs through the year 2010. The following year, PSWAC submitted a report containing recommendations for the improvement of public safety communications over wireless networks. *Final Report of the Public Safety Wireless Advisory Committee*, September 11, 1996.

Appendix I - Federal Administration

The lead federal program for fostering interoperability is administered by the Wireless Public SAFEty Interoperable COMmunications Program, dubbed Project SAFECOM,[63] part of the Department of Homeland Security. The key federal agencies for spectrum management in first responder communications are the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). Among other responsibilities, the FCC supervises spectrum for non-federal public safety agency communications. The NTIA—part of the Department of Commerce—administers spectrum used by federal entities. SAFECOM has not to date played a major role in spectrum policy. DHS has created an Office of Interoperability and Compatibility (OIC) of which SAFECOM is a part. In June 2004 DHS announced the creation of a Regional Technology Integration Initiative. DHS has also announced the organization of a National Incident Management System (NIMS) in response to a Presidential Directive (HSPD-5).[64] A NIMS Integration Center is planned to deal with compatibility and could be responsible for at least some interoperable communications.

National Telecommunications and Information Administration

To address the need for interoperability spectrum, in June 1999 the NTIA designated certain federally-allocated radio frequencies for use by federal, state, and local law enforcement and incident response entities. The frequencies are from exclusive federal spectrum, and are adjacent to spectrum used by state and local governments. NTIA's "interoperability plan,"—developed in coordination with the Interdepartmental Radio Advisory Committee (IRAC)[65]—is used to improve communications in response to emergencies and threats to public safety. In 1996, the NTIA created a public safety program to coordinate federal government activities for spectrum and telecommunications related to public safety. Today, its successor, the Public Safety Division of the Office of Spectrum Management, participates in various initiatives to improve and coordinate public safety communications. The Division is preparing a *Spectrum Efficiency Study* and an *Interoperable Communications Summary Guide*.[66] Two forums on public safety and spectrum use have been sponsored by the NTIA, one in June 2002 and another in February 2004.[67]

[63] Additional information is at [http://www.safecomprogram.gov/SAFECOM/].

[64] Full document at [http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf]. Viewed October 13, 2005.

[65] IRAC, with representation from 20 major federal agencies, develops policies for federal spectrum use, and represents the United States at International Telecommunications Union conferences. See [http://www.ntia.doc.gov/osmhome/irac.html]. Viewed October 13, 2005.

[66] Additional information at [http://ntiacsd.ntia.doc.gov/pubsafe/]. Viewed JOctober 13, 2005.

[67] Agenda and reports of the 2004 Public Safety Forum are available at [http://www.ntia.doc.gov/ntiahome/ntiageneral/specinit/forum2/]. Viewed October 13, 2005.

Federal Communications Commission

Over roughly the last 20 years, the FCC has initiated several programs that involve state, local, tribal and—usually—private sector representatives. In 1986, it formed the National Public Safety Planning Advisory Committee to advise it on management of spectrum in the 800 MHZ band, newly designated for public safety. The following year, the FCC adopted a Public Safety National Plan that, among other things, established Regional Planning Committees (RPC) to develop plans that met specific needs. The FCC encourages the formation of RPCs with a broad base of participation. The RPCs have flexibility in determining how best to meet state and local needs, including spectrum use and technology.

The regional planning approach is also being applied to spectrum in the Upper 700 MHz band.[68] Technical and operational standards, including interoperability standards, were developed and recommended to the FCC through the Public Safety National Coordination Committee (NCC). Standards for narrowband radio applications, for example, were recommended to the FCC and adopted in early 2001. Established by the FCC in 1999 and ended in 2003, the NCC had a Steering Committee from government, the public safety community, and the telecommunications industry.

Homeland Security. After Hurricane Katrina, the FCC established a panel to examine the impact of Hurricane Katrina and make recommendations to the FCC regarding actions it might take to improve public safety operations, disaster preparation, and network reliability.[69] The independent panel is holding meetings and soliciting comments regarding events during and after the hurricane and what changes in communications infrastructure might be considered. The FCC has also notified Congress of its plans to establish a Public Safety and Homeland Security Bureau within the agency. The new bureau would have responsibility for coordinating public safety, homeland security, and disaster management activities at the FCC.[70]

Among past actions by the FCC specifically in support of homeland security were the chartering of the Media Security and Reliability Council (MSRC)[71] and the renewal of the charter for the Network Reliability and Interoperability Council (NRIC).[72] Both of these are Federal Advisory Committees. MSRC has been active in evaluating the effectiveness of the Emergency Alert System. The primary role of NRIC is to develop recommendations for best practices for private sector telecommunications to insure optimal reliability, interoperability, and connectivity

[68] See [http://wireless.fcc.gov/publicsafety/700MHz/]. Viewed October 11, 2005.

[69] FCC News, "Chairman Kevin J. Martin Names Nancy J. Victory as Chair of the Federal Communications Commission's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks," November 28, 2005 at [http://www.fcc.gov].

[70] FCC News, "FCC Adopts Plan to Establish a Public safety and Homeland Security Bureau," March 17, 2006 at [http://www.fcc.gov].

[71] See [http://www.fcc.gov/MSRC/Welcome.html]. Viewed October 13, 2005.

[72] See [http://www.nric.org].

of networks. The current NRIC focus groups are: Near Term Issues, E911; Long Term Issues, E911; Best Practices, E911 and Public Safety; Emergency Communications Beyond E911; Best Practices, Homeland Security - Infrastructure; Best Practices, Homeland Security - CyberSecurity; Best Practices, Wireless Industry; Best Practices, Public Data Networks; and Broadband.

Spectrum and Interoperability. The FCC's strategic goal for spectrum is to "Encourage the highest and best use of spectrum domestically and internationally in order to encourage the growth and rapid deployment of innovative and efficient communications technologies and services."[73]

Regarding interoperability, the FCC describes its role as "directing efforts toward allocating additional spectrum for public safety systems, nurturing technological developments that enhance interoperability and providing its expertise and input for interagency efforts such as SAFECOM."[74] However, the FCC asserts that there are limitations on what it can do. "The Commission is only one stakeholder in the process and many of the challenges facing interoperability are a result of the disparate governmental interests . . . making it difficult to develop and deploy interoperable strategies uniformly."[75]

Department of Homeland Security

National Response Plan. The National Response Plan lays out organization charts for authority and responsibility in Incidents of National Significance and after the declaration of a disaster or an emergency. One of the key players for emergency communications is the National Communications System (NCS). The primary role of NCS is to assure federal communications and the integrity of certain vital networks, such as for banking. It also is prepared to assist in recovery and restoration of service for commercial and emergency services. The NCS has no significant role in providing emergency communications support for first responders. The job of coordinating communications is assigned by the National Response Plan to the Federal Emergency Communications Coordinator. As described in the plan, the power of this position to command and deliver needed communications support is limited, and in any event, it occurs after the fact.

Office of Interoperability and Compatibility. The function of the Office of Interoperability and Compatibility (OIC) is to address the larger issues of interoperability. Among the goals of the OIC is the "leveraging" of "the vast range of interoperability programs and related efforts spread across the Federal Government" to "reduce unnecessary duplication" and "ensure consistency" in

[73] See [http://www.fcc.gov/omd/strategicplan/#goals]. Viewed October 13, 2005.

[74] Testimony of John B. Muleta, Chief, Wireless Telecommunications Bureau, Federal Communications Commission at Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "More Time, More Money, More Communication?," September 8, 2004.

[75] Ibid.

"research and development, testing and evaluation (RDT&E), standards, technical assistance, training, and grant funding related to interoperability." To achieve this, DHS will create within OIC "a series of portfolios to address critical issues." The OIC's initial priorities are for communications (SAFECOM), equipment, training and "others as required." To fulfill the portfolios, OIC will use a "systems engineering or lifestyle approach" to create "action plans." These will be "developed through a collaborative process that brings together the relevant stakeholders to provide clear direction on a path forward." This "end-user" input is expected to produce "a strategy and action plan" for each portfolio.[76] No time line for accomplishing these planned steps has of yet been provided,

SAFECOM. With the support of the Administration, Project SAFECOM was designated the umbrella organization for federal support of interoperable communications. It was agreed within DHS that SAFECOM would be part of the Science and Technology Directorate, in line with a policy for placing technology prototype projects under a single directorate; this decision was reportedly based on the research-oriented nature of the programs envisioned for SAFECOM by its administrators.[77] The Intelligence Reform and Terrorism Prevention Act affirmed this decision by giving DHS the authority to create an office for interoperability within the Science and Technology Directorate and to manage SAFECOM as part of that effort.[78] SAFECOM has released a template for interoperability planning that can be used by states to establish a strategy for interoperability[79] and is preparing a methodology to establish a baseline for interoperability achievements as an evaluation tool to measure the success of future interoperability programs. SAFECOM expects to release initial findings on the baseline measurement some time in 2006.[80]

SAFECOM absorbed the Public Safety Wireless Network (PSWN) Program, previously operated jointly by the Departments of Justice and the Treasury. PSWN was created to respond to recommendations made by the Public Safety Wireless

[76] Testimony of Dr. David G. Boyd, Program Manager, SAFECOM and Deputy Director, Office of Systems Engineering & Development, Science and Technology Directorate, Department of Homeland Security, Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, "Public Safety Interoperability: Look Who's Talking Now," July 20, 2004.

[77] "Homeland Security Starting Over With SAFECOM," *Government Computer News*, June 9, 2003.

[78] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (a) (2).

[79] Statewide Communication Interoperability Planning (SCIP) Methodology, SAFECOM Program, Directorate of Science and Technology, Department of Homeland Security at [http://www.safecomprogram.gov/SAFECOM/library/interoperabilitycasestudies/1223_statewidecommunications.htm]. Viewed February 2, 2006.

[80] Oral testimony of Dr. David G. Boyd, Program Manager, SAFECOM and Deputy Director, Office of Systems Engineering & Development, Science and Technology Directorate, Department of Homeland Security, at hearing, House of Representatives, Committee on Energy and Commerce, "Public Safety Communications from 9/11 to Katrina: Critical Public Policy Lessons," September 29, 2005.

Advisory Committee regarding the improvement of public safety communications over wireless networks. PSWN operated as an advocate for spectrum management policies that would improve wireless network capacity and capability for public safety. SAFECOM, however, has no authority over spectrum management decisions. The following quote is a summary of SAFECOM's position on spectrum policy.

> Spectrum policy is an essential issue in the public safety communication arena. Unfortunately, State and local public safety representatives are frequently not included in spectrum policy decisions, despite their majority ownership of the communications infrastructure and their importance as providers of public and homeland security. SAFECOM will hence play a role in representing the views of State and local stakeholders on spectrum issues within the Federal Government. Last year, SAFECOM was appointed to an interagency Spectrum Task Force to contribute such views, and the ongoing working relationship that has developed between SAFECOM and the FCC will, we believe, pay huge dividends in the future.[81]

SAFECOM was chosen in October 2001 as one of 24 e-government initiatives. It was categorized as a government-to-government initiative in the original strategizing for e-government programs.[82] When SAFECOM was created in 2001, the managing partner for SAFECOM was the Department of the Treasury. Subsequently, the program was assigned to the Federal Emergency Management Agency (FEMA), following FEMA when it moved to the Emergency Preparedness and Response Directorate of the Department of Homeland Security (DHS). Once at DHS, SAFECOM was assigned to the Directorate of Science and Technology. As the Government Accountability Office (GAO) has noted in testimony and reports,[83] the change in leadership has delayed progress at SAFECOM. The GAO has also expressed concern over a lack of leadership and focus and raised questions of governance. Testimony by David Boyd[84] has stressed the importance to SAFECOM of more authority in certain funding decisions and in its interactions with other federal agencies, and the need for an in-depth gap analysis—the assessment of current levels of interoperable communications capability compared to requirements.

[81] Boyd, Hearing, July 20, 2004.

[82] Office of Management and Budget, *Implementing the President's Management Agenda for E-Government: E Government Strategy*, February 27, 2002, p.13.

[83] For example, U.S. Government Accountability Office, *Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO Report GAO-04-963T (Washington: July 20, 2004); and U.S. Government Accountability Office, *Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders*, GAO Report GAO-04-1057T (Washington: September 8, 2004).

[84] Testimony of Dr. David G. Boyd, Program Manager, SAFECOM and Deputy Director, Office of Systems Engineering & Development, Science and Technology Directorate, Department of Homeland Security, Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, "Public Safety Interoperability: Look Who's Talking Now," July 20, 2004 and Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "More Time, More Money, More Communication?," September 8, 2004.

The GAO has recommended that the Director of the Office of Management and Budget work with DHS to review SAFECOM's functions and establish a long-term program with appropriate authority and funding to coordinate interoperability efforts across the federal government.[85]

Other notable observations from the GAO include:

- The fragmented federal grant structure for first responders does not support statewide interoperability planning. SAFECOM has developed grant guidance for interoperability, but cannot require that consistent guidance be incorporated in all federal first responder grants.
- The federal government can provide the leadership, long-term commitment, and focus to help state and local governments meet interoperability goals. For example, the federal government can provide the leadership and support for developing (1) a national database of interoperable communications frequencies, (2) a common nomenclature for those frequencies, (3) a national architecture that identifies communications requirements and technical standards, and (4) statewide interoperable communications plans.[86]

SAFECOM, however, articulated a different approach in testimony and its 2003 Strategy Planning Session. In its strategy summary, it reported that it intends, over the course of 10 to 20 years, to "Adopt a national strategy from the bottom up to incorporate effective public safety communications."[87] Boyd also reaffirmed his belief that "any effort to improve communications interoperability must be driven from the bottom up."[88] This approach necessitates a focus on communications at the incident level. At this level, SAFECOM appears to be giving the greatest attention to improving radio interoperability, particularly through the deployment of cross-talk hardware. This decision in turn leads to an emphasis on increasing the amount of equipment standardization, improving operating standards and protocols, and consulting on how to install and use new equipment. According to Boyd's testimony, the focus for SAFECOM is on three areas: creation of an architectural framework, the development of standards, and the coordination of federal activities.[89] The architectural framework is intended to aid SAFECOM in determining priorities for the development of standards. The framework "will reflect a system-of-systems approach to develop interface standards to help improve the problem of

[85] U.S. General Accountability Office, *Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders*, GAO Report GAO-04-1057T (Washington: September 8, 2004).

[86] Ibid.

[87] SAFECOM Strategy Planning Session," Executive Summary, May 2003 Findings, p. 4.

[88] Boyd testimony, September 8, 2004.

[89] Ibid.

communications interoperability."[90] It appears that it will be modeled along the lines of a pyramid, with decision-making starting at the base and building up. The organic nature of the SAFECOM model for infrastructure development apparently requires a long time-line (usually extending, in testimony, to 20 years) and resists description in terms of long-term goals and deadlines. By describing its achievements and plans within the framework of short-term milestones, many of which involve the preparation of studies by outside consultants, SAFECOM appears to have avoided addressing many of the strategic goals originally envisioned for its mission, without an official explanation for the shift in emphasis.

SAFECOM Strategy as an E-Government Initiative. In 2002 and 2003, OMB sequentially described SAFECOM's mission, milestones and goals. It appears that many of these goals have not been met, or have been modified. The 2002 E-Government Strategy document described SAFECOM's mission as follows:

> For public safety officials to be effective in their daily responsibilities, as well as before, during and after an emergency event, public safety agencies throughout all levels of government, i.e. federal, state and local, must be able to communicate with each other. This initiative would address the Nation's critical shortcomings in efforts by public safety agencies to achieve interoperability and eliminate redundant wireless communications infrastructures. At the same time, it would assist state and local interoperability and interoperability between federal public safety networks.
> Value to Citizen: Coordinated public safety/law enforcement communication will result in saved lives, as well as better-managed disaster response. Consolidated networks will yield cost savings through reduction in communication devices, management overhead of multiple networks, maintenance and training.
> Value to the Government: Billions of dollars could be saved through a right-sized set of consolidated, interoperable federal networks, linked to state wireless networks, resulting in a reduction in communications infrastructure, overhead, maintenance and training.[91]

Milestones - 2002. In February 2002, SAFECOM milestones, all planned for completion by the end of that year, included the following:

- Define the communications concept of operations for interaction that identifies the communications requirements to address the two highest probable threat scenarios: Bio terrorism and natural disasters.
- Develop an integrated public safety response solution that addresses the top two threat scenarios by using existing infrastructure augmented by available commercial capability.
- Complete a gap analysis of existing inventories of public safety wireless communications at federal, state and local level.[92]

[90] Ibid.

[91] Office of Management and Budget, *Implementing the President's Management Agenda for E-Government: E Government Strategy*, February 27, 2002, p. 30.

[92] Ibid., p. 15.

Goals - 2003. In the April 2003 E-Government Strategy Report, the immediate (2003) goals for SAFECOM were restated, as follows:

- Define the requirements for first responder interoperability at state, local, tribal, and federal levels to develop a long-term architecture.
- Identify gaps between existing wireless systems and interoperability requirements.
- Develop national architecture
- Develop concept of operations for interoperability.[93]

Many Goals Not Met. Comparing the stated goals of SAFECOM as an e-government program, with its current progress and programs, it appears that the emphasis has been on short-term goals. There is virtually no indication, in testimony, of long-term planning for national interoperability. Among its accomplishments, SAFECOM has partly met the goal of developing a requirements statement with the qualitative assessment of communications needs at the incident level, as provided in the March 2004 "Requirements" document. A gap analysis is reportedly underway, a delivery date of late 2005[94] has been extended to mid-2006.[95] The "concept of operations" for "interaction" (2002) or "interoperability" (2003) could be equated with the pyramid structure advocated by SAFECOM, discussed below, and this may provide the framework for an "integrated public safety response solution." An integrated response solution and a national architecture are promised for the future.[96] The 2002 milestone of providing a plan to use "existing infrastructure augmented by available commercial capability" is being addressed if infrastructure is defined as local radio communications equipment bolstered by cross-patch hardware. It is not being met, and seems to have been rejected by SAFECOM, if infrastructure is meant to include wide-area networks, Internet communications backbones and other regional or national communications capacity that would provide broad-based communications the support.

In testimony,[97] OMB described SAFECOM goals as including the provision of "interoperable wireless solutions for Federal, state, and local public safety organizations," that would include "coordination of all Federal interoperability

[93] Office of Management and Budget, *Implementing the President's Management Agenda for E-Government: E Government Strategy*, April 2003, p. 30.

[94] U.S. Department of Homeland Security, Fact Sheet: Achieving First Responder Communications Interoperability—a Local, State and Federal Partnership, at [http://www.dhs.gov/dhspublic/].

[95] Oral testimony of Dr. David G. Boyd, Program Manager, SAFECOM and Deputy Director, Office of Systems Engineering & Development, Science and Technology Directorate, Department of Homeland Security, Hearing of the House of Representatives, Committee on Energy and Commerce, "Public Safety Communications from 9/11 to Katrina: Critical public Policy Lessons," September 29, 2005.

[96] *Boyd testimony, September 8, 2004.*

[97] *November 6, 2003 Statement of Karen Evans,* Testimony before a subcommittee of the House Committee on Government Reform, 108th Cong., 1st sess. (Hereafter cited as *November 6, 2003 Evans Statement*.)

efforts." In OMB's description of long-term strategic goals, as outlined in the 2003 e-gov plan, there appears to be an implicit assumption that there are redundant wireless communications infrastructures that can be identified and eliminated. This planning document describes the SAFECOM initiative as addressing "critical shortcomings," including two significant points where communications interoperability is lacking; interoperability between *state and local* authorities, as well as interoperability between *federal* public safety networks. The plan indicates that some (unidentified) networks would be consolidated to yield costs savings. Further "Billions of dollars" in savings are presumed by creating a right-sized set of consolidated, interoperable federal networks, linked to state wireless networks. To date, there appears to be no information on SAFECOM plans for improving wireless communications networks at the national or regional level; the focus of the program on hardware solutions at the incident level would seem to preclude plans for network interoperability or the establishment of standards for new interoperable technologies such as mesh networks or cognitive radios. Work at the incident level is primarily local, focused on short-range interoperability solutions. Wide area networks and nationwide, end-to-end communications rely on technologies not being tested or evaluated by SAFECOM at the incident level.

In particular, the build-from-the-bottom-up approach for interoperability, advocated by SAFECOM, would appear to be at odds with the e-government goal of achieving efficiencies at the communications network level. Modern networks, with their incorporation of software programs on chips, other software-programmable technologies, nanotechnology, and meshed communications systems, to cite some examples, are generally built out from a common design, requiring some degree of centralization. In that respect, the goals of the IWN appear to be more aligned to the original goals of the e-government strategy. Its intentions include the construction of a national network, the identification and prioritization of end-user functional requirements, and the use of open standards that would be adapted by other public safety agencies.

Evolution of SAFECOM's Goals. The explanation of SAFECOM provided in 2002 by OMB,[98] would suggest that the original mission was much broader than the milestones that have been used to chart progress. It is possible, therefore, that SAFECOM has not merely suffered delays because of changes in the managing partner, as the GAO has observed,[99] but also because it has changed course, redefining its purpose.

Regional Technology Integration Initiative

In June 2004, the Directorate of Science and Technology introduced a new initiative to facilitate the transition of innovative technologies and organizational

[98] Office of Management and Budget, *Implementing the President's Management Agenda for E-Government: E Government Strategy*, February 27, 2002, p.30.

[99] U.S. General Accountability Office, *Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO Report GAO-04-740 (Washington: July 2004).

concepts to regional, state, and local authorities.[100] The initiative has selected four urban areas from among those currently part of the Homeland Security Urban Area Security Initiative. Two of the areas that have been reported as choices are Cincinnati, Ohio and Anaheim, California.[101] Each area will reportedly receive $10 million to expand new systems that test more advanced technologies for public safety communications, including interoperability. Anaheim, for example, reportedly has created a virtual operations center (instead of a building), relying on network technology to connect police, fire, medical services and public utilities in case of an emergency. The announced goal is to get all who respond to disasters and other emergencies to work from a common base.[102]

National Incident Management System (NIMS)

NIMS also has announced plans to address questions of interoperability and communications, although no mention of spectrum policy is mentioned in the DHS report on NIMS issued March 1, 2004.[103] The objective for communications facilitation is summarized as "development and use of a common communications plan and interoperable communications processes and architectures."[104] NIMS envisions mandatory compliance with "national interoperable communications standards, once such standards are developed."[105] These standards will include interoperable wireless communications for "Federal, State, local and tribal public safety organizations."[106]

Integrated Wireless Network

The Integrated Wireless Network (IWN) for law enforcement is being planned as a joint program by the Departments of Justice, the Treasury, and Homeland Security. DHS is represented in the IWN Joint Program Office through the Wireless Management Office of the Chief Information Officer.[107] IWN, from its description,

[100] DHS Press Releases, including "Homeland Security Launches Regional Technology Integration Initiative in Seattle," February 18, 2005 [http://www.dhs.gov/dhspublic/display?content=4362] and "Fact Sheet: Regional Technology Initiative" at [http://www.dhs.gov/dhspublic/display?theme=43&content=3704]. Viewed September 13, 2005

[101] "Department of Homeland Security funding initiative aims to spur interoperability among locals," by Jim McKay, Government Technology, September 2004, p. 1.

[102] Ibid.

[103] "National Incident Management System," Department of Homeland Security, March 1, 2004, at [http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf]. Viewed September 14, 2005

[104] Ibid., p. 11.

[105] Ibid., p. 50.

[106] Ibid., p. 52.

[107] Memorandum of Understanding Between the Department of Homeland Security, the Department of Justice, and the Department of the Treasury Regarding a Joint Tactical

(continued...)

will have limited interoperability at the state and local level. The described objective of IWN is network integration for “the nation’s law enforcement wireless communication, and data exchange capability through the use of a secure integrated wireless network.”[108]

National Communications System

The National Communications System is assigned responsibility for telecommunications under the Secretariat of Information Analysis and Infrastructure Protection within DHS.[109] It was originally within the Department of Defense, established by Executive Order in 1984 “to assist the President ... in 1) the exercise of the telecommunications functions and responsibilities, and (2) the coordination of the planning for and provision of national security and emergency preparedness communications...” It consults with the National Security Telecommunications Advisory Committee (NSTAC), among others, on issues related to national security and emergency preparedness telecommunications. It is closely linked to the White House through NSTAC, which advises the President on national security telecommunications matters, and the National Security Council.[110]

Its primary functions for National Security and Emergency Preparedness are to assure critical telecommunications access for selected federal and state agencies, to coordinate restoration of service with the private sector, and to establish priorities in the restoration of service. Among its services in time of disaster, NCS operates the National Coordinating Center (NCC) for Telecommunications—which coordinates public and private sector efforts to restore telecommunications—and manages an Individual Mobilization Augmentee program to in bring civilian and military reservists to assist recovery efforts.[111]

Other Coordinating Bodies

SAFECOM has created a Federal Interoperability Coordination Council (FICC), made up of “all the federal agencies with programs that address interoperability.”[112] Previously, as part of its e-government mandate to rationalize federal programs for interoperability, SAFECOM met with representatives from 60 different programs operated by the federal government or funded by or partnered with a federal agency. Many of these programs include state committees and national associations such as the Association of Public-Safety Communications Officials - International

[107] (...continued)
Wireless Communications System, at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

[108] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.3 (a), page 8 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed October 13, 2005.

[109] Homeland Security Act of 2002, P.L. 107-296, Sec. 201 (e) (19) (g) (2).

[110] See [http://www.ncs.gov].

[111] See [http://www.ncs.gov/services.html].

[112] Boyd testimony, September 8, 2004.

(APCO).[113] Part of the National Coordination Committee's mission was to encourage the creation of Statewide Interoperability Executive Committees (SIEC),[114] to take part in coordination efforts. The National Public Safety Telecommunications Council (NPSTC) is another important coordinating body. NPSTC unites public safety associations to work with federal agencies, the NCC, SIECs and other groups to address public safety communications issues.[115] It has been supported by the AGILE Program, created by the National Institute of Justice (NIJ).[116] AGILE has addressed interim and long-term interoperability solutions in part by testing standards for wireless telecommunications and information technology applications. The AGILE Program also has provided funding to Regional Planning Committees for start-up costs and the preparation and distribution of regional plans. AGILE has been restructured, replaced by a more limited function in Communications Technology, CommTech. CommTech is not designed to play a primary role in coordinating interoperability policy within the public safety community.

The SIECs, NPSTC, Regional Planning Committees and other federally-supported but not federally-directed organizations play key roles as facilitators in advancing programs for public safety communications. In recent testimony quoted above,[117] both SAFECOM and the FCC have described their roles primarily as facilitators also. SAFECOM and DHS, in its plans for the Office of Interoperability and Compatibility, seem to place a high priority on consultative functions. It appears that OIC policy will focus on portfolios of recommendations for achieving interoperability at an incident site and not on establishing the higher levels of interoperability provided by network support and back-up from regional communications command centers. In its discussions of Emergency Operations Centers and Incident Command Systems, however, NIMS seems to indicate the need for a national network architecture and fixed as well as mobile operations centers for communications network support. The Regional Technology Integration Initiative has been established to Act as a catalyst between existing technology used by first responders and the innovative technology needed in the future. It seeks to work at the local, state and regional levels but appears to favor solutions that can be applied on a regional basis.

[113] See [http://www.apcointl.org/].

[114] A discussion of the role of SIECs, and a recommendation to mandate their use, is contained in testimony by Stephen T. Devine, Missouri SIEC Chairperson, Missouri State Highway Patrol, at Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, "Public Safety Interoperability: Look Who's Talking Now," July 20, 2004.

[115] Information at [http://npstc.org].

[116] AGILE stands for Advanced Generation of Interoperability for Law Enforcement. See [http://www.ojp.usdoj.gov/nij/topics/commtech/]. Viewed January 4, 2006.

[117] Boyd and Muleta, Hearing, July 20, 2004.